REAL PARTY IN INTEREST

The real party in interest is Aurora Wireless Technologies, Ltd., which has full title to the present application by virtue of an assignment from the inventors recorded on July 3, 2002 at Reel/Frame No. 013084/0100.

RELATED APPEALS AND INTERFERENCES

There are no appeals or interferences that will directly affect, be directly affected by, or have a bearing on the Board's decision in this appeal.

STATUS OF CLAIMS

Claims 1-28 are pending in the application. Claims 1-26 stand finally rejected and rejected two or more times. Claims 27-28 have been withdrawn from consideration. The rejections of claims 1-26 are appealed.

STATUS OF AMENDMENTS

No amendments were filed and/or not entered after the Final Office Action was mailed on June 11, 2008 and before the filing of this Appeal Brief.

SUMMARY OF CLAIMED SUBJECT MATTER

The present invention relates generally to user authentication for network communications and transactions, and particularly to a network infrastructure for providing user authentication that employs biometrically controlled private keys. According to some aspects, the invention allows networked businesses and merchants such as financial institutions to ensure that user authentication is conducted in a trusted, secure fashion within standard network environments.

For example, public key cryptography and public key infrastructures (PKI) are known methods for providing secured on-line transactions in network environments. As is known, public key cryptography includes the use of asymmetric public keys and private keys (i.e. key pairs). PKI may further include the use of digital certificates and certification authorities. For example, as illustrated in Figure 1 of the present application, when a sender 102 wishes to send a

trusted message to recipient 104 (e.g. for a secure transaction), sender 102 applies for a key pair from certificate authority 106. Certificate authority (CA) 106 creates a key pair comprising a private key 108 and a public key 110 for sender 102. The CA further issues an encrypted digital certificate 114 containing the sender's public key and a variety of other identification information. The CA makes its own public key 112 available through, for example, print publicity or on the Internet. The intended recipient 104 can then use the CA's public key 112 to decode the digital certificate and verify that it was issued by the CA 106. With this information, the recipient can then obtain the sender's public key 110 and use it to send an encrypted reply back to sender 102. A message from sender 102 to recipient 104, whether encrypted or not, can also include a digital signature for further verification. As is known, the digital signature is generated from the message itself using the sender's private key 108, verifying that the signature belongs to this particular message, and thus assuring that the contents of the message have not been tampered with. Using sender's public key 110, the recipient 108 can thus decode the digital signature and perform such additional verification.

In one example implementation, as shown in Figure 2 of the present application, the invention uses a combination of biometric technology to control access to access private keys and to create digital signatures based on biometric authentication and existing PKI technologies. According to another aspect of the invention, the system includes a client/server design that works seamlessly in a network environment. In one possible example, the system includes an authentication server that has access to biometric templates required to authenticate an individual before accessing the user's own private key, and the ability to route digital signatures to appropriate downstream entities for transaction processing. This includes entities such as payment gateways, financial institutions, or other authentication brokers. The invention employs biometrics user authentication as well as private key infrastructure technologies. In embodiments, the invention stores private key(s) on a secure server to which access is granted for a requested transaction only after a biometric signature has been validated (for example a fingerprint).

In furtherance of these and other aspects, independent claim 1 sets forth a method comprising: storing a private key (e.g. private key 206) associated with a user at an authentication server (e.g. PKdl server 212, Figure 2, page 10, lines 10-15), receiving a request

for access to a service from the user (e.g. page 16, lines 11-15); collecting a biometric sample from the user (e.g. page 12, lines 7-16) via a client associated with the user (e.g. PKdI client 220) and remote from the authentication server on a network (e.g. page 10, line 16 to page 11, line 9); sending the collected biometric sample from the client to the authentication server (e.g. page 14, line 19 to page 15, line 7); comparing, at the authentication server, the biometric sample to a biometric template (see Figure 3) associated with the user (e.g. page 14, line 19 to page 15, line 7); and if a result of the comparing step indicates a match between the biometric sample and template for the user: allowing the private key from the authentication server to be accessed and used with the request (e.g. page 16, lines 16-21); encrypting the request with the private key (e.g. page 16, lines 16-21), and providing the service with access to a public key (e.g. public key 204) corresponding to the private key (e.g. page 10, lines 5-9), wherein access to the private key stored at the authentication server for use in encrypting the user's request is prevented unless and until the authentication server determines that the user's collected biometric sample that was sent by the client matches the biometric template (e.g. page 8, line 20 to page 10, line 9).

Similarly, independent claim 14 sets forth an apparatus comprising: means for storing a private key (e.g. private key 206) associated with a user at an authentication server (e.g. PKdl server 212, Figure 2, page 10, lines 10-15), means for receiving a request for access to a service from the user (e.g. page 16, lines 11-15); means for collecting a biometric sample from the user (e.g. page 12, lines 7-16) via a client associated with the user (e.g. PKdl client 220) and remote from the authentication server on a network (e.g. page 10, line 16 to page 11, line 9); means for sending the collected biometric sample from the client to the authentication server (e.g. page 14, line 19 to page 15, line 7); means for comparing the biometric sample to a biometric template (see Figure 3) associated with the user (e.g. page 14, line 19 to page 15, line 7); and if a result of the comparing means indicates a match between the biometric sample and template for the user: means for allowing the private key from the authentication server to be accessed and used with the request (e.g. page 16, lines 16-21); means for encrypting the request with the private key (e.g. page 16, lines 16-21), and means for providing the service with access to a public key (e.g. public key 204) corresponding to the private key (e.g. page 10, lines 5-9), wherein access to the private key stored at the authentication server for use in encrypting the user's request is prevented unless and until the authentication server determines that the user's collected biometric

sample that was sent by the client matches the biometric template (e.g. page 8, line 20 to page 10, line 9).

In additional furtherance of the above and other aspects of the invention as set forth in claim 5, which depends from claim 4, the method of claim 1 further includes providing a biometric signature (e.g. signature 208) corresponding to the collected biometric sample to the service associated with the request (e.g. page 17, lines 3-13), and allowing the service to determine whether to fulfill a transaction corresponding to the request in accordance with the result of the comparing step (e.g. page 21, line 19 to page 22, line 6).

Similar to claim 5, claim 18, which depends from claim 17, the apparatus of claim 14 further includes means for providing a biometric signature (e.g. signature 208) corresponding to the collected biometric sample to the service associated with the request (e.g. page 17, lines 3-13), and means for allowing the service to determine whether to fulfill a transaction corresponding to the request in accordance with the result of the comparing means (e.g. page 21, line 19 to page 22, line 6).

In additional furtherance of the above and other aspects of the invention as set forth in claim 10, which depends from claim 9, the method of claim 1 further includes decrypting the encrypted biometric sample at the authentication server (e.g. page 15, line 8 to page 16, line 7); and checking the integrity information included with the biometric sample (e.g. page 15, line 8 to page 16, line 7).

Similar to claim 10, as set forth in claim 23, which depends from claim 22, the apparatus of claim 14 further includes means for decrypting the encrypted biometric sample at the authentication server (e.g. page 15, line 8 to page 16, line 7); and means for checking the integrity information included with the biometric sample (e.g. page 15, line 8 to page 16, line 7).

In yet additional furtherance of the above and other aspects of the invention as set forth in claim 6, the method of claim 1 further includes generating pre-enrollment keys for the user and supplying the pre-enrollment keys to respective key generators (e.g. page 17, line 18 to page 18, line 9); and generating a final enrollment key for the user only if keys provided by a key administrator match the pre-enrollment keys supplied to the key generators, the key administrator being a person different than the key generators (e.g. page 18, lines 10-17).

Similar to claim 6 as set forth in claim 19, the apparatus of claim 14 further includes means for generating pre-enrollment keys for the user and means for supplying the pre-enrollment keys to respective key generators (e.g. page 17, line 18 to page 18, line 9); and means for generating a final enrollment key for the user only if keys provided by a key administrator match the pre-enrollment keys supplied to the key generators, the key administrator being a person different than the key generators (e.g. page 18, lines 10-17).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

In the Final Office Action, claims 1-5, 9-18 and 22-26 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,678,821 to Waugh et al. ("Waugh").

Claims 6-8 and 19-21 stand rejected under 35 U.S.C. 103(a) as being obvious over Waugh in view of U.S. Patent No. 4,652,698 to Hale ("Hale") and U.S. Patent No. 7,188,362 to Brandys ("Brandys").

Appellants respectfully submit that all of these rejections are in error for multiple reasons, and seek review of the following independently reversible grounds:

- Whether Waugh by itself teaches the inventions of independent claims 1 and 14.
- Whether Waugh by itself teaches the inventions of dependent claims 5 and 18.
- Whether Waugh by itself teaches the inventions of dependent claims 10 and 23.
- Whether the alleged combination of Waugh, Hale and Brandys would have suggested the inventions of dependent claims 6 and 19.

ARGUMENT

Waugh Does Not Anticipate Independent Claims 1 and 14

The following ground for reversal applies to claims 1-5, 9-18 and 22-26. Of these claims, claims 1 and 14 are independent, with the other claims depending directly or indirectly therefrom.

Appellants respectfully submit that Waugh does not meet the requirements for anticipation under 35 U.S.C. §102. More particularly, Appellants note that a cited prior art reference anticipates a claimed invention under the statute only if every element of the claimed

invention is identically shown in the single reference. MPEP §2131; *In re Bond*, 910 F.2d 831, 832, 15 USPQ 2d 1566, 1567 (Fed. Cir. 1990). Each and every limitation of the claim is significant and must be found in the single cited prior art reference. *In re Donohue*, 766 F.2d 531, 534, 226 USPQ 619, 621 (Fed. Cir. 1985). Moreover, the test for anticipation by a single reference under 35 USC § 102 requires that the single reference not only disclose all elements of the invention, but that the elements be "arranged or combined in the same way as in the claim". *Net MoneyIN, Inc. v. VeriSign, Inc.*, __ F.3d __ (Fed. Cir. 2008) .

Independent claims 1 and 14 require, *inter alia*:

> [a] storing a private key associated with a user at an authentication server;
>
> [b] collecting a biometric sample from the user via a client that is remote from an authentication server on a network;
>
> [c] sending the collected biometric sample from the client to the server;
>
> [d] comparing, at the server, the collected sample to a biometric template associated with the user;
>
> [e] if the comparison results in a match, encrypting the user's request for a service with a private key and providing a corresponding public key to the service; and
>
> [f] wherein access to the private key from the server is prevented unless and until the authentication server determines that the collected sample sent by the client matches the template.

For reasons set forth more fully below, the process taught by Waugh operates in a completely different manner than the claimed inventions and therefore does not teach or suggest them.

<u>Waugh Does Not Teach Or Suggest Comparing A Collected Biometric Sample At An Authentication Server</u>

Waugh teaches that when a user wants to encrypt a message to send to another user, she downloads an ID template from a server 28 to a client computer, obtains a fingerprint sample at the client computer, and <u>the client computer</u> compares the fingerprint with the template . If there is sufficient correspondence between the sample and the template, a private key that is <u>already</u>

provided to the client in the ID template is released from the ID template for use by the client computer in encrypting the message. (col. 4, line 65 to col. 5, line 34).

Accordingly, it is clear that Waugh does not teach or suggest at least elements [c], [d] and [f] as set forth above, which require the collected sample to be sent to the server, and for the server to perform a comparison and to prevent access to the private key until a match is determined.

In the Final Office Action, the Examiner makes several statements in response to the facts provided above. However none of these statements demonstrates that Waugh, by itself, teaches all the express limitations of the claims, as is required for a § 102 rejection.

First, the Examiner poses the question : "is 'sending the collected biometric sample from the client to the authentication server and comparing, at the authentication server, the biometric sample to a biometric template associated with the user' not well known in the art?" (Action at 3.) This question and its answer are inapposite because the Examiner has chosen to rely on Waugh alone as anticipating all the elements of the claimed invention. Accordingly, the burden is on the Examiner to prove that all claim limitations are expressly or impliedly taught by Waugh alone. The Examiner has failed to do that, as shown above. In any event, Appellants respectfully submit that the inventions as completely set forth in the claims are not taught or suggested by the cited prior art.

The Examiner next refers to a telephone conversation with Appellants' representative on October 25, 2007. This conversation occurred as a result of an unsolicited telephone call from the Examiner three days before the mailing of the Office Action in which Waugh was first cited, and for which there is no Interview Summary. To the extent the Final Office Action is providing an Interview Summary, Appellants respectfully submit that it is inaccurate, and the only prior art discussed in that call was the cited prior art of record at that time. In any event, it is irrelevant, because all claim limitations must be taught or suggested by Waugh, which they are not as shown above.

Next, the Examiner refers to a Wikipedia definition of "server" and suggests that a server can be a software/application. The Examiner also argues that Waugh shows that "server" functionality for performing biometric comparison is transferred to the client computer. Apparently, the Examiner is trying to show that Waugh's "server" can be in the same device as

Waugh's "client." Again, this is irrelevant, because the claims clearly require that the client that collects the biometric sample is remote from an authentication server on a network. Accordingly, the server that performs the comparison and prevents access to the private key must be remote from the client on a network. On the contrary, Waugh clearly teaches that the biometric sample collection and comparison is performed in the same physical computer.

The clear differences between the claimed invention and Waugh's teachings are neither trivial nor obvious. Even though it is encrypted, Waugh clearly provides access to the private key by the client computer before biometric authentication. As such, any unauthorized person using the client computer can attempt to hack the private key offline indefinitely, which can result in the private key being compromised.

Waugh Does Not Teach Or Suggest Providing A Corresponding Public Key To A Service

The Final Office Action also fails to show how Waugh teaches or suggests providing, to the service requested by the user, a public key corresponding to the private key if the comparison between the collected sample and template indicates a match, as required by [e] of claims 1 and 14 as set forth above.

For this clearly defined subject matter, the Final Office Action points to step 108 in Fig. 4, col. 5, lines 44-53, and claims 1 and 2. At best, these disclosures of Waugh merely teach using a private key to encrypt or decrypt messages. Nowhere does Waugh teach or suggest, in these passages or elsewhere, providing a corresponding public key to a service that the user is requesting.

For at least the above reasons, independent claims 1 and 14 patentably define over Waugh, and the § 102 rejections thereof should be reversed, together with the § 102 rejections of claims 2-5 and 9-13 that depend from claim 1, and claims 15-18 and 22-26 that depend from claim 14.

<u>Waugh Does Not Anticipate Dependent Claims 5 And 18</u>

The following ground for reversal applied to claims 5 and 18. Claim 5 ultimately depends from claim 1 and claim 18 ultimately depends from claim 14 and thus claims 5 and 18 are allowable for at least the reasons claims 1 and 14 are allowable.

Claims 5 and 18 also depend from claims 4 and 17, respectively. Both claims 5 and 18 further require:

> [g] providing a biometric signature corresponding to the collected biometric sample to the service requested by the user; and
>
> [h] allowing the service to determine whether to fulfill a transaction corresponding to the request in accordance with the result of the comparison between the collected biometric sample and the template.

The Examiner relies on col. 5, lines 7-12 and step 108 in Figure 4 of Waugh as teaching the above subject matter. These passages merely state that an <u>ID template</u> downloaded by the client contains a biometric standard 82 and a digital identifier 88 (note that the text of Waugh sometimes incorrectly uses reference numeral 84 to refer to the digital identifier 88 shown in Figure 4) . The standard 82 is used to compare against the collected fingerprint, and the private key is extracted from the identifier 88 if there is a sufficient match. The private key can then be used to encrypt a message for the user <u>at the client computer</u>. These passages do not mention anything about providing anything corresponding to the <u>collected biometric sample</u>.

More importantly, nowhere in these passages or elsewhere does Waugh teach or suggest a <u>biometric signature</u> corresponding to a collected biometric sample <u>at all</u>, much less providing such a signature to a service that a user is requesting, and then allowing that service that receives the signature to further determine whether to fulfill a transaction corresponding to the user's request.

For at least these additional reasons, claims 5 and 18 further patentably define over Waugh and the § 102 rejections thereof should be reversed.

Waugh Does Not Anticipate Dependent Claims 10 And 23

The following ground for reversal applied to claims 10 and 23. Claim 10 ultimately depends from claim 1 and claim 23 ultimately depends from claim 14 and thus claims 10 and 23 are allowable for at least the reasons claims 1 and 14 are allowable.

Claims 10 and 23 also depend from claims 9 and 22, respectively. Both claims 10 and 23 further require:

> [g] encrypting the collected biometric sample for transmission to the authentication server;
>
> [h] including integrity information in the encrypted biometric sample;
>
> [i] decrypting the encrypted biometric sample at the authentication server; and
>
> [j] checking the integrity information included with the biometric sample.

The Examiner relies on col. 5, lines 22-33 and claim 1 of Waugh as teaching the above subject matter. These passages merely state that an ID template downloaded by the client contains a biometric standard 82 and a digital identifier 88. The standard 82 is used to compare against the collected fingerprint, and the private key is extracted from the identifier 88 if there is a sufficient match.

Nowhere in these passages or elsewhere does Waugh teach or suggest <u>encrypting or decrypting</u> a collected biometric sample <u>at all</u>, much less providing such a signature to a service that a user is requesting, and then allowing that service that receives the signature to further determine whether to fulfill a transaction corresponding to the user's request.

For at least these additional reasons, claims 5 and 18 further patentably define over Waugh and the § 102 rejections thereof should be reversed.

Waugh, Hale And Brandys Would Not Have Suggested Claims 6 and 19

Claims 6-8 and 19-21 stand rejected under §103 based on an alleged combination of Waugh with Hale and Brandys. Claim 6 ultimately depends from claim 1, and claim 19 ultimately depends from claim 14. Claims 7-8 depend from claim 6 and claims 20-21 depend from claim 19. The rejections of claims 6-8 and 19-21 should be withdrawn for at least the

reason that Hale and Brandys do not cure the deficiencies of Waugh discussed above and, consequently, no combination of the cited art teaches all elements of claims 6-8 and 19-21.

Furthermore, even if combined as alleged in the Final Office Action, Waugh, and Hale and Brandys do not meet certain elements and limitations of the claims as alleged by the Office Action. For example, claims 6 and 19 further require:

> [g] generating pre-enrollment keys for the user;
>
> [h] supplying the pre-enrollment keys to respective key generators;
>
> [i] generating a final enrollment key for the user only if keys provided by a key administrator match the pre-enrollment keys supplied to the key generators, the key administrator being a person different than the key generators.

The Examiner relies on Hale's Abstract as teaching the above subject matter. However, this passage merely describes a process of allowing a user to access a desired file from a central processor. Nowhere does Hale teach or suggest anything about generating a final enrollment key by a key administrator based on a comparison with pre-enrollment keys by different respective kcy generators.

The Final Office Action states that claims must be interpreted as broadly as reasonable. Appellants agree. However, it is respectfully submitted that no <u>reasonable</u> person of ordinary skill would interpret Hale's disclosure of numbers and algorithms used to retrieve desired files from a central processor as suggesting a process of generating a final enrollment key by a person designated as a key administrator as clearly set forth in claims 6 and 19.

Therefore, for at least these reasons, the §103 rejections should be reversed.

CONCLUSION

For the foregoing reasons, Appellants respectfully request that all the pending claims be deemed allowable by this honorable Board.

Respectfully submitted,
PILLSBURY WINTHROP SHAW PITTMAN LLP

Date: December 9, 2008

Mark J. Danielson 40,580
Reg. No.

Telephone: (650) 233-4777
Facsimile: (703) 770-7901
Please reply to customer no. 27,498

CLAIMS APPENDIX

1. (Previously presented) A method comprising:

storing a private key associated with a user at an authentication server;

receiving a request for access to a service from the user;

collecting a biometric sample from the user via a client associated with the user and remote from the authentication server on a network;

sending the collected biometric sample from the client to the authentication server;

comparing, at the authentication server, the biometric sample to a biometric template associated with the user; and

if a result of the comparing step indicates a match between the biometric sample and template for the user:

allowing the private key from the authentication server to be accessed and used with the request;

encrypting the request with the private key, and

providing the service with access to a public key corresponding to the private key,

wherein access to the private key stored at the authentication server for use in encrypting the user's request is prevented unless and until the authentication server determines that the user's collected biometric sample that was sent by the client matches the biometric template.

2. (Previously presented) A method according to claim 1, further comprising:

if the result indicates a match, generating a digital signature using the private key for use with the request.

3. (Original) A method according to claim 2, further comprising:

providing the digital signature to the service associated with the request.

4. (Original) A method according to claim 1, further comprising:
providing a biometric signature corresponding to the collected biometric sample to the service associated with the request.

5. (Original) A method according to claim 4, further comprising:
allowing the service to determine whether to fulfill a transaction corresponding to the request in accordance with the result of the comparing step.

6. (Original) A method according to claim 1, further comprising:
generating pre-enrollment keys for the user;
supplying the pre-enrollment keys to respective key generators; and
generating a final enrollment key for the user only if keys provided by a key administrator match the pre-enrollment keys supplied to the key generators, the key administrator being a person different than the key generators.

7. (Previously presented) A method according to claim 6, further comprising:
verifying registration of the user in accordance with a validation of the final enrollment key;
creating the biometric template for the user only if registration is verified; and
generating the private key only if the biometric template is successfully created.

8. (Original) A method according to claim 6, further comprising associating user identification information with the final enrollment key.

9. (Previously presented) A method according to claim 1, further comprising:
encrypting the collected biometric sample for transmission to the authentication server; and
including integrity information in the encrypted biometric sample.

10. (Original) A method according to claim 9, further comprising:
decrypting the encrypted biometric sample at the authentication server; and

checking the integrity information included with the biometric sample.

11. (Original) A method according to claim 9, wherein the integrity information includes a unique transaction identifier.

12. (Previously presented) A method according to claim 1, further comprising:
associating user identification information with the private key; and
maintaining a digital certificate containing the user identification information and the public key corresponding to the private key at the authentication server.

13. (Original) A method according to claim 1, wherein the biometric sample includes a fingerprint scan.

14. (Previously presented) An apparatus comprising:
means for storing a private key associated with a user at an authentication server;
means for receiving a request from the user for access to a service;
means for collecting a biometric sample from the user via a client associated with the user and remote from the authentication server on a network;
means for ending the collected biometric sample from the client to the authentication server;
means for comparing the biometric sample to a biometric template associated with the user; and
if a result of the comparing means indicates a match between the biometric sample and template for the user:
means for allowing the private key from the authentication server to be accessed and used with the request;
means for encrypting the request with the private key, and
means for providing the service with access to a public key corresponding to the private key,
wherein access to the private key stored at the authentication server for use in encrypting the user's request is prevented unless and until the authentication server determines

that the user's collected biometric sample that was sent by the client matches the biometric template.

15. (Previously presented) An apparatus according to claim 14, further comprising:
if the result indicates a match, means for generating a digital signature using the private key for use with the request.

16. (Original) An apparatus according to claim 15, further comprising:
means for providing the digital signature to the service associated with the request.

17. (Original) An apparatus according to claim 14, further comprising:
means for providing a biometric signature corresponding to the collected biometric sample to the service associated with the request.

18. (Original) An apparatus according to claim 17, further comprising:
means for allowing the service to determine whether to fulfill a transaction corresponding to the request in accordance with a result of the comparing means.

19. (Original) An apparatus according to claim 14, further comprising:
means for generating pre-enrollment keys for the user;
means for supplying the pre-enrollment keys to respective key generators; and
means for generating a final enrollment key for the user only if keys provided by a key administrator match the pre-enrollment keys supplied to the key generators, the key administrator being a person different than the key generators.

20. (Previously presented) An apparatus according to claim 19, further comprising:
means for verifying registration of the user in accordance with a validation of the final enrollment key;
means for creating the biometric template for the user only if registration is verified; and
means for generating the private key only if the biometric template is successfully created.

21. (Original) An apparatus according to claim 19, further comprising means for associating user identification information with the final enrollment key.

22. (Previously presented) An apparatus according to claim 14, further comprising:
means for encrypting the collected biometric sample for transmission to the authentication server; and
means for including integrity information in the encrypted biometric sample.

23. (Original) An apparatus according to claim 22, further comprising:
means for decrypting the encrypted biometric sample at the authentication server; and
means for checking the integrity information included with the biometric sample.

24. (Original) An apparatus according to claim 22, wherein the integrity information includes a unique transaction identifier.

25. (Previously presented) An apparatus according to claim 14, further comprising:
means for associating user identification information with the private key; and
means for maintaining a digital certificate containing the user identification information and the public key corresponding to the private key at the authentication server.

26. (Original) An apparatus according to claim 14, wherein the biometric sample includes a fingerprint scan.

27. (Withdrawn) An authentication infrastructure comprising:
a server that intercepts a request by a user for access to a service and controls access to a stored private key associated with the user; and
a client that collects a biometric sample from the user in response to the user making the request and sends the collected biometric sample to the server,
wherein the server maintains a biometric template associated with the user for authenticating the collected biometric sample, and
wherein, if and only if the collected biometric sample matches the biometric template:

the server allows access to the stored private key for use in encrypting the request, so that the user need not maintain a token for accessing the service, and the user need not store the private key, and

the server provides the service with access to a public key corresponding to the private key,

wherein access to the private key stored at the server for use in encrypting the user's request is prevented unless and until the authentication server determines that the user's collected biometric sample that was sent by the client matches the biometric template.

28. (Withdrawn) An authentication infrastructure according to claim 27, wherein the private key is further used to sign a message for allowing the user to perform the transaction with the service, the service obtaining the corresponding public key from the server.

EVIDENCE APPENDIX

NONE

RELATED PROCEEDINGS APPENDIX

NONE